Notice of Allowability	Application No.	Applicant(s)	
	09/721,398	ENGLAND ET AL.	
	Examiner	Art Unit	
	Jacob F. Betit	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the after final amendment filed 18-February-2005*.

2. ☒ The allowed claim(s) is/are *1-16,18-22,30-33,36-39,41,44,46-52,54-56,62,63 and 71-78*.

3. ☒ The drawings filed on *22 November 2000* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

SAM RIMELL
PRIMARY EXAMINER

DETAILED ACTION

Remarks

1. In response to communications filed on 18-February-2005, claims 1, 18-19, 36, 38, 41, 46, 52, and 54-55 per applicant's request. Claims 1-16, 18-22, 30-33, 36-39, 41, 44, 46-52, 54-56, 62-63, and 71-78 are presently pending in the application.

Allowable Subject Matter

2. Claims 1-16, 18-22, 30-33, 36-39, 41, 44, 46-52, 54-56, 62-63, and 71-78 allowed.

3. The following is an examiner's statement of reasons for allowance:

The prior art of record does not disclose, teach or suggest:

wherein the plurality of instructions further cause the one or more processors to perform acts including:

mapping a central processing unit reset vector to an initialization vector;

receiving a read request corresponding to the central processing unit reset vector from one of the one or more central processing units;

returning, in response to the read request, the initialization vector to the one central processing unit; and

allowing the one central processing unit to access the memory beginning with the initialization vector, as claimed in claim 1.

Claims 2-16, 18-22, and 71-74 are allowable over the prior art of record because they are dependent on allowed independent claim 1.

The prior art of record does not disclose, teach or suggest:

initiating secure execution of the trusted core by:

mapping a central processing unit reset vector to an initialization vector;

resetting each of the one or more central processing units in the computer;

receiving, after the mapping and resetting, a read request corresponding to the central processing unit reset vector from one of the one or more central processing units;

returning, in response to the read request, the initialization vector to the one central processing unit; and

allowing the one central processing unit to access the memory beginning with the initialization vector, as claimed in claim 30.

Claims 31-33 are allowable over the prior art of record because they are dependent on allowed independent claim 30.

The prior art of record does not disclose, teach or suggest:

initiating execution of the additional code in a secure manner despite the untrustworthy code in the computer;

mapping a central processing unit reset vector to an initialization vector;

receiving a read request corresponding to the central processing unit reset vector from one central processing unit;

returning, in response to the read request, the initialization vector to the one central processing unit; and

allowing the one central processing unit to access the memory beginning with the initialization vector, as claimed in claim 36.

Claims 37-39, 41, and 44 are allowable over the prior art of record because they are dependent on allowed independent claim 36.

The prior art of record does not disclose, teach, or suggest:

a controller, coupled to the memory protector portion, to:

map a processor reset vector to an initialization vector;

receive a read request corresponding to the processor reset vector from the processor;

return, in response to the read request, the initialization vector to the processor; and

allow the processor to access the memory beginning with the initialization vector, as claimed in claims 46 and 62.

Claims 47-52, 54-56, and 75-78 are allowable over the prior art of record because they are dependent on allowed independent claim 46.

Claim 63 is allowable over the prior art of record because they are dependent on allowed independent claim 62.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. patent No. 5,867,655 to DeRoo et al. for teaching using a single EEPROM to store firmware for a CPU, firmware for the SCP, and the system password and other critical data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (571) 272-4075. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (571) 272-4083. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
25 Mar 2005

SAM RIMELL
PRIMARY EXAMINER